Appendix Y
Threat Considerations for Testing

Y–1. Overview of threat considerations in testing

Army policy requires that testing include an accurate representation of the threat projected to exist at a system post-initial operational capability (IOC) date. Threats must be identified, approved, and updated continuously throughout the system's life cycle (AR 381–11). DIA-approved threat or system-specific threat definitions developed in accordance with appropriate regulations will be employed when tests are planned, designed, and conducted.

Y–2. Management of the threat during test planning

a. Testers are expected to understand the evolving threat and integrate it into tests that address COIC or exit criteria, AI, or technical characteristics and are realistic, representative, and credible. Threat-related issues should be managed using the following guidelines:

b. Coordination between testers and the system evaluator with the appropriate MACOM threat support organization (usually the TRADOC center or school threat manager) responsible for the production of the STAR and Threat TSP should be established early and continue throughout test planning.

c. In addition to the approved COIC, the supporting threat organization must have access to the AI and the planning data embodied in the test design concept in the SEP. The test design includes the scope (that is, tactical scenarios, degree of operational realism, and types of test events), test factors and conditions (that is, control of factors to ensure test events occur under appropriate combinations of test conditions), and test design matrices (that is, grouping of test conditions into trials, vignettes, missions, and phases). Without this information, the TRADOC Threat Manager (TM), who is drafting the Threat TSP, will not be able to properly shape the threat to meet the objectives of the test. This will result in a Threat TSP that is less than adequate to do the job and could result in the TISO (from HQDA DCS, G–2) pulling the threat validation from the test.

d. Since the Threat TSP supports preparation of the EDP and DTP some of the interrelationships between the documents begins to emerge. The Threat TSP must be prepared to meet regulation-specified test planning timelines. The supporting threat organization must receive test design data as early as possible. This all begins with the activities of the Threat Coordination Group (TCG).

Y–3. Threat Coordination Group

The system specific TCG should be stood up immediately after the formation of the T&E WIPT. (See para 5–14*b*.) It is the mission of the TCG to focus and refine the threat found in the STAR into the threat requirements for the test(s). This can only be accomplished in a timely manner if the five key players (Threat Officer, TSM, Evaluator, Tester, and PM) coordinate early, continuously, provide the information requested, and have a clear understanding of the inter-relationship that each has to the other for mission accomplishment. Once at least some of the threat requirements can be ascertained and locked by the TCG, then and only then is it time to stand up the Threat Accreditation Working Group (TAWG). The TCG is also responsible for ensuring the adequacy of the threat resources as they are represented in the TEMP. If available, the most current threat validation report will be used to assist in determining the adequacy of threat resources to represent the desired threat. Note that there is only one official report that looks at the overall adequacy of a threat—the validation report. The Threat will continue to evolve and mature with time. That is why it is imperative that the TCG ensure the latest DIA validated threat assessments for all test specific threat requirements are reviewed and carefully considered for incorporation in all threat related documentation.

Y–4. Threat Accreditation Working Group (TAWG)

After at least some of the threat requirements for the test(s) have been identified and locked by the TCG the TAWG is formed to accredit specific test application of threat simulators, targets, surrogates, and target arrays. The TAWG operates to approve these threat requirements and convert them into accredited threat resources for a specific test application(s). When available, applicable threat system validation reports are used to assist in determining the overall threat worthiness of threat test resources. Included in its membership are representatives from the same organizations that comprise the TCG as well as representatives of PM ITTS, threat simulator and target materiel developer offices, appropriate Intelligence Production Center analyst(s), and the MATDEV. The TAWG should meet at least 24 months prior to the test (T–720) in order to have adequate time to accomplish the following functions:

a. Ensure that the threat requirements identified and locked by the TCG are compared to the threat resources in the TEMP. Any changes must be clearly identified and documented.

b. Ensure that this new list of threat resources can be used to replicate the desired threat using actual threat articles,

surrogates, simulators, or simulations. Where they cannot, this must be clearly documented as a test limitation and its impacts assessed and reported in the Threat TSP or its accompanying Threat System Accreditation Report (TSAR).

c. For OT, ensure that threat resources documented in the final OTP reflect threat requirements identified by the TCG and that can be accredited by the TAWG are what is submitted to the TSARC for approval prior to the test. This will give a true reflection of the actual threat costs for the test, showing availability, accreditation potential, and requirement fulfillment.

d. Accredit the use of designated threat simulators/targets for each test.

e. Identify differences ("deltas") between the simulators or targets and current estimates of corresponding threat system characteristics and assess their impacts on the test.

f. Through comparison of the drafts of the Threat TSP and the SEP, accreditation offers a timely opportunity to reconcile differences between them. Also, this facilitates development of test planning guidance as a basis to complete the SEP and provide increased assurance that the threat resources identified are sufficient to represent the threat with greater fidelity during the test.

Y–5. Threat in Test Readiness Reviews

TRADOC is responsible for validating the planned threat portrayal. For tests including force-on-force trials, TRADOC also validates the threat force training plan prepared by the TM. For OT, this validation is documented in the OTRS prepared by the CBTDEV. The ATEC Threat Support Activity (ATSA) also participates to report of the preparedness of threat simulators.

Y–6. Deviations from the threat

When significant deviations from the validated threat are expected in test portrayals, whether due to a lack of threat resources or situations dictated by testing requirements, and/or it is determined that potential portrayal shortfalls pose significant risks to test validity, the appropriate TM and threat integration center should be consulted as soon as these are identified so they can seek "offsets" or alternatives to minimize potential threat-related test limitations. The TRADOC Threat Manager (TM) must be forthright and inform the testers and evaluators where deviations can and cannot be accommodated. The TM should immediately notify TRADOC ADCSINT Threats, T&E Division for assistance. As required TRADOC should seek formal HQDA (DCS, G–2) Threat Integration Staff Officer (TISO) recommendations for any alternative solutions that may have been missed to permit early resolution of problems. Once the Threat TSP has been finalized and approved by HQDA (DCS, G–2) and for OSD T&E Oversight programs, reviewed and concurred with by DIA, deviations become much more problematic. Testers and evaluator must be able to clearly articulate to the threat intelligence community why these deviations are necessary and work with them to find an acceptable solution that will not result in the validity of the threat portrayal to be compromised.

Y–7. Threat portrayal fidelity

Due to resource limitations (availability of threat systems in the quantity, fidelity, and diversity sometimes required), it is unlikely that the threat force in a test will be represented with total fidelity to the threat as described in the STAR, especially in OT, nor is it really expected to. What is expected is that the threat requirements identified and locked in the TCG process, accredited in the TAWG process, and documented in the Threat TSP and its accompanying TSAR that have been specifically designed for the test will be represented with total fidelity. This however, is not always the case. The degree to which threat force operations will be faithfully represented during the test will be based on subjective judgments of the TRADOC TM and the level of training of the threat system operators.

Y–8. Threat critiques

Intelligence personnel supporting or observing test preparations and/or execution should direct commentary or critiques on the threat portrayal through the evaluator. These critiques and commentary should be as specific as possible and include the significance of the comment or critique to the overall threat portrayal during that trial or vignette. It is the responsibility of both the Intelligence Representative and the Evaluator to come to an agreement as to the significance. This will ensure that only those comments deemed relevant to the interpretation and evaluation of test results are communicated to other personnel directly associated with the test.

Y–9. Resolution of threat shortfalls

Normally, the CBTDEV and MATDEV who are responsible for the STAR and Threat TSP, assist in setting up the test and overseeing its threat-related aspects. The Army validating authority for threat portrayals, will be on-site and is capable of interpreting the significance of threat-related issues on test validity, thereby minimizing the potential for controversy.

Y–10. Threat test limitations

Significant portrayal shortfalls must be included in test reports as "test limitations" and their impact on test validity assessed in T&E reports.

Y–11. Threat is dynamic and uncertain

The threat to be portrayed in testing results from an intelligence estimative analytical process that assesses specific military capabilities of a potential enemy usually at future point in time. Although uncertainty is inherent in all intelligence, estimative intelligence, due to the limited availability of collectable information, to a greater degree than other types of analytical disciplines, is heavily reliant on applied methodologies usually derived from the physical sciences. As new intelligence is developed and intelligence gaps narrow or close as a result of supplemental collection and analysis or evolving methodologies, the threat may change. If the DA TCG determines these changes to be substantial, they must be incorporated into T&E activities.

Y–12. Threat in test planning

The STAR is used to define the tactical context to support development of the TEMP, OTP, and the SEP.

Y–13. Threat Test Support Package

The Threat TSP is a document (or set of documents) that provides a description of the threat against which the new system will be tested. It is required for all materiel programs. Derived from the STAR, the Threat TSP is more detailed and is used in developing the test environment necessary to prepare the final SEP and provides the threat scenarios for each operational test. Determination of the threat year and scenario selection for the test will be made by the T&E WIPT upon the recommendation of the MATDEV and the system evaluator. The development of the Threat TSP (both initial and final) cannot be done in a vacuum. It takes close coordination between and amongst all the principal participants (TM, Tester, Evaluator, TSM) to ensure that nothing becomes disjointed. Each of the principal participants has an important function. Evaluator provides the initial drafts of the SEP, MOPs, MOEs, and Failure Definition Scoring Criteria. The tester provides the initial drafts of the test concept to include the terrain over which the test will be conducted. The TSM provides the overall capabilities and limitations of the system and the concerns of the Combat Developer. As each of these is refined and matured they are provided to the TM and potential impacts, changes are discussed and agreed to. An initial Threat TSP is developed immediately after MS A to support future testing for a specific system or concept.

a. The Threat TSP defines the threat portion of a realistic operational test environment adequate to test the developmental system in the context of related COIC or exit criteria and AI.

b. Preparation and Approval.

(1) To support DT requirements, the MATDEV/PM (that is, threat support organization) will expand and tailor the initial Threat TSP for each test for which threat force operations are to be portrayed realistically. It is here that the STAR is critical. Since the STAR outlines all the known threats to the system undergoing test, it provides DT with unique insights to potential vulnerabilities that are not limited to the geo-political realities of one threat country or region.

(2) For OT, the CBTDEV, normally the TRADOC proponent center/school TM, prepares the initial Threat TSP for each IOT, 18 months (T–540) before the test start date. This date is not hard and firm. Rather, it is flexible based upon the needs of the system undergoing test; and the availability of information required to construct the document. The due dates for both the initial and final Threat TSP should be coordinated and approved in one of the first meeting of the T&E WIPT. For other tests (FDT/E, EUT, LUT, or FOT), a Threat TSP will be prepared unless the T&E WIPT acting upon the recommendation of the system evaluator, determines that a validated threat portrayal is not required for the test. The requirements of the COIC OTDC, and TEMP will form the basis for a recommendation to waive the Threat TSP.

(3) For user testing of tactical systems, the threat integration center, usually the TRADOC ADCSINT Threats, T&E Division, approves/validates the Threat TSP, from a tester's perspective, to ensure that threat operations are portrayed accurately and consistently. DA DCS, G–2 is the validation authority for Threat TSPs for ACAT I, ACAT II, and ACAT III systems on the OSD T&E Oversight List and provides a copy to DIA for review and comment. Most Threat TSP for OT of other Non-major systems are approved and validated by the TRADOC ADCSINT Threats, T&E Division, while this is done by appropriate AMC FIO, when a Threat TSP is required to support DT. The Final Threat TSP to include all appendices is dependent upon the coordinated completion of the test trials and vignettes (coordination between Tester, Evaluator, TSM, and TM) and the Threat System Accreditation Report. The Final Threat TSP must be approved and validated 12 months before the test date (T–365), or as coordinated in the T&E WIPT for the system undergoing test.

c. The Threat TSP format and content is detailed in appendix C, AR 381–11. It is prepared in modular format to facilitate the updating process from test to test since only those parts required for a given test need to be completed. Section III (Threat) of the Threat TSP often requires revision, since the AI and the SEP continue to evolve.

d. When approved, the Threat TSP describes the threat to be used for planning and developing the test and to be portrayed during test execution. An approved Threat TSP, however, does not ensure that test threat portrayal is valid. Two separate approval actions are required, one for the Threat TSP and one for the threat portrayal during the test. The approved threat is included in the SEP prior to testing.

Y–14. Integration of threat data in operational test planning and threat and evaluation measures of effectiveness and measures of performance

Although the system evaluator has access to threat intelligence (for example, STAR) shortly after program initiation that is used to define the tactical context for the test, actual integration of the threat into OT does not begin until after completion of the functional dendritics, which do not consider the threat. The dendritics for each system are used to define system functions and subfunctions, clarify primary MOE derived from the COIC, and formulate MOP and data requirements necessary for OT. Even though the functional dendritics do not take into account the threat when they are used to formulate the MOP and MOE; the formulation of the MOP and MOE are essential in the identification of the Threat Requirements for a given test. MOP and MOE are used as limiting factors in determining both the threat that is required (system types and capabilities) and the threat that although a viable threat to the system undergoing test has no bearing upon the outcome of this particular test.

Y–15. Test factors and conditions for threat

Threat becomes operative as the system evaluator endeavors to identify factors (that is, test variables likely to effect test event outcomes) and the conditions (that is, discrete aspects of a factor, or factors, often expressed as a range of values, capabilities, or operational modes). Threat data (such as the types and echelon of forces, types and numbers of systems, and doctrine and tactics) which determine threat force movements and operations under varying situations, become factors and conditions for purposes of developing a test concept. Once these determinations are made, usually through use of a matrix approach keyed to each COIC, the system evaluator then must decide how each factor and condition, including those related to the threat, will be controlled during testing (that is, "fixed," "systematically varied," "tactically varied," or "uncontrolled").

Y–16. Threat and the tactical context

The STAR is used to define the tactical context describing the threat environment and threat systems that will exist at the IOC date and throughout the life cycle of the developmental system. The evaluator uses the STAR and information developed in the TCG process to identify the tactical setting as well as develop the factors and conditions to formulate the "test approach" section of the SEP. The system evaluator must make this same information available to the appropriate threat support office, usually the TRADOC center/school TM, as early as possible, in order to expedite preparation of the Threat TSP, which is essential to development of the SEP. As the tester refines the test approach guidance developed by the evaluator, must continue coordination with the TM to ensure timely completion of a Threat TSP tailored to test requirements.

Y–17. Threat and the operational test environment

The OT environment is the "Force-on-Force" application of the Defense Planning Guidance scenario in an OT (combat situation). Once the T&E WIPT, based upon the recommendations of TRADOC ADCSINT Threat, T&E Division, determines the most appropriate Defense Planning Guidance TRADOC standard scenario to be used in the test, the TCG core members (DIA and supporting IPC, DA DCS, G–2, and TRADOC ADCSINT Threats) craft the threat operational environment or combat situations in which the system will be tested at the post IOC time (usually IOC + 10 years). The combined effects of the combat situations in the force on force ("blue" vs. "red") create a unique opportunity to measure the combined and cumulative effects of both enhancing and diminishing factors on the test.

a. Enhancing factors. The "blue" organization, TTPs, and doctrine of employment are integrated so that operational effectiveness of the system is enhanced.

b. Diminishing factors. At the same time, a system's operational effectiveness is subjected to diminishing factors. The chief diminishing factor standing between the system and the achievement of its mission is the "red" organization, TTPs, and doctrine of employment. Others factors include the effects of weather, terrain, and interference from other systems.

Y–18. Threat in the developmental test environment

Within DT, the tester and evaluator are free to run the gambit of all threats as outlined in the STAR without regard to country of origin or the impacts of any existing or projected political-military realities. This affords the tester and evaluator the ability to truly stress the system under test. This allows for the creation of a true worst case scenario and environment where the most lethal threats real and projected from a host of countries can be combined and there combined effects measured.

Y–19. Test profile

Threat TSPs contain threat profiles, system profiles, and environmental profiles. Test designers merge threat, system, and environmental profiles into test profile sets that are incorporated into the SEP.

Y–20. Threat profiles

The Threat TSP contains individual test threat profiles consistent with the overall test objectives, scenarios, and threat resources to be used. Threat profiles describe the types of threat and threat equipment that the system is likely to

encounter, specific threat effects anticipated, threat tactics and countermeasures, threat doctrine and employment practices, and threat organizations. The operational tester uses the threat profiles to develop the OT environment and the target arrays for the test.

Y–21. Scoping of threat in test profiles

Because the number of possible test profile sets is so large and COIC can be resolved through analytical means other than OT, it is neither economical nor desirable to develop threat profiles for every possible profile set. Therefore, the tester must monitor the preparation of the Threat TSP closely to ensure that threat profiles are—

a. Configured appropriately for the environmental conditions and means of employment (tactics, doctrine, and organization) that are most important in order to respond to the test issues.

b. Developed only for those aspects of a threat profile that are technically possible, operationally feasible, and realistic.

Y–22. Threat profile complexity

Because the Threat TSP becomes progressively more complex during the system development process, test threat profiles also increase correspondingly in scope and complexity.

a. For EUT, the test threat profiles focus on potential targets, countermeasures, and opposing weapons at the single system one-on-one level.

b. For IOT&E, the test threat profiles, depending on the developmental system, can expand to include opposing forces up to the battalion level.

c. At FOT&E, the test threat profiles include an updated configuration of potential opposing forces at all levels.

Y–23. Threat scenarios

a. Defense Planning Guidance. The annual Defense Planning Guidance, issued by the Secretary of Defense, provides a set of common planning assumptions for U.S. and friendly forces and planning scenarios projected for a ten-year period. It also defines strategy and force options identifying the specific operational environments in which U.S. forces must be prepared to function. The Defense Planning Guidance is also the basis for development of U.S. Army scenarios to support the force and materiel development processes.

b. TRADOC standard scenarios. The purpose of a standard scenario is to provide consistency and reduce bias for all combat development programs through use of a common base case that portrays TRADOC-approved U.S. Army doctrinal and operational concepts. The TRADOC Analysis Command is the proponent for scenario development for friendly forces, while TRADOC ADCSINT Threats, T&E Division, assists in preparation of the threat force scenario, which is validated by HQDA (DCS, G–2). TRADOC standard scenarios are considered in the development of threat force scenarios in the Threat TSP and preparation of the Integrated Threat Tactical Operations Plan, both of which support the test design process. During OTP preparation/preliminary test design planning, the system proponent and the operational tester, based upon recommendations from TRADOC ADCSINT Threats, T&E Division and subject to T&E WIPT approval, select the standard scenario for use in testing. Both friendly and threat test operations must be compatible with the selected standard scenario. It is this Defense Planning Guidance based scenario that serves as the backdrop for the test. With the test trials and vignettes (snapshots in time out of the chosen Defense Planning Guidance based TRADOC scenario) being carefully selected for their operational context and their ability to properly frame each portion of the test.

c. Integrated Threat Tactical Operations Plan. The Integrated Threat Tactical Operations Plan is an instructional guide for the operation of simulators also useful in test planning, specifically as a reference in preparing both the SEP and the detailed test plan (DTP). It is produced by ATSA, approved by ATEC, and validated by HQDA.

Y–24. Threat depiction in environmental profiles

These profiles define the terrain, weather, communications, and transportation infrastructures, friendly interference (for example, radio frequency), time and distance separating operating forces from their support structure, and other non-threat conditions under which the test is to be conducted. The test environmental profiles are drawn from the system requirements documents and supporting analyses.

Y–25. Threat adequacy

a. The COIC may require measurement of the combined impact of the factors that enhance and diminish operational effectiveness on lethality and survivability or the multiplying effect of one system on the lethality and survivability of another system. When either circumstance exists, the operational tester and system evaluator with the assistance of the TRADOC ADCSINT Threats, T&E Division must ensure that the threat portrayed in the test will be sufficient to support the system evaluation of direct effect systems as well as the impacts of indirect effect systems.

b. Lacking an adequate threat portrayal that considers both types of systems, the evaluator will be unable to make accurate assessments of system operational effectiveness.

Y–26. Threat and modeling and simulation

Threat considerations in employing M&S may be based on the following—

a. Threat-related resource limitations. Estimated threat capabilities cannot be adequately represented due to a lack of threat simulators/targets and/or threat surrogates that match estimated threat capabilities.

b. Uncertainties and variables. M&S techniques have considerable potential for improving the fidelity of the portrayal of threat in OT activities. There are significant uncertainties related to the estimates of future threat capabilities that should be carefully considered in all OT activities. Sensitivity analyses, using M&S techniques, can be applied to examine the impacts of incomplete or uncertain estimative intelligence on testing. In addition, M&S can assist in projecting the implications of future enemy reactive threat to the system being tested. Typical aspects of the threat that lend themselves to M&S techniques include—

(1) System performance characteristics, for which intelligence production centers (IPCs) develop their best estimates that normally become the basis for OT design, as well as high and low parametric values as a means of "bounding" the uncertainties.

(2) Variables related to evolving threat forces as a result of materiel upgrades, organizational changes, and modifications of doctrine and TTP.

(3) Scenario-related operational options involving the types of combat operations being portrayed (for example, main attack versus supporting attacks, or offense versus defense).

c. Pretest M&S applications.

(1) An important use of M&S techniques in test planning is the refinement of test scenarios and data matrices to decide which elements of system performance should be the focus of OT. To do this, the M&S used must relate the operational effectiveness and suitability of the system in a realistic scenario, with appropriate force levels using situations identified in the OMS/MP. This allows the system evaluator to do sensitivity, contingency, and functional analyses for various technical and force mix assumptions.

(2) There is a perceived need in designing tests to compare (or determine the differences or "deltas") between the performance of threat simulators/targets deployed in the test array and evolving intelligence estimates of the characteristics and capabilities of the actual threat system(s).

Y–27. Threat support to model-test-model concept

Although there are rigorous VV&A procedures for the application of M&S techniques in OT, an essential prerequisite for their use is a process to ensure that threat representations and usage modeled or simulated are consistent with approved estimative intelligence through Army and Defense Intelligence Agency (DIA) validation.

a. Approval/validation of threat data. The threat represented in the model must be documented and traceable to an approved and validated STAR and Threat TSP, or to automated threat data from other approved Army high- and low-resolution models. The threat portions of M&S developed by TRADOC are approved by TRADOC ADCSINT Threats, T&E Division and validated by HQDA (DCS, G–2). Threat data to be used in M&S applications, however, are validated by TRADOC ADCSINT Threats, T&E Division. Deviations from threat data contained in HQDA (DCS, G–2) and DIA approved intelligence, however, must be fully documented and approved by HQDA (DCS, G–2) before use.

b. Threat requirements for sensitivity analyses. If M&S is appropriate to conduct sensitivity analyses related to uncertainties in the threat, the system evaluator will require a range of threat alternatives or variables (that is, threat force weapons and systems parameters and/or doctrinal, organizational, or operational options derived by intelligence analysts).

Y–28. Accreditation of Threat Input to M&S used in T&E

Just as Threat Simulators and Targets must be accredited to determine their appropriateness and suitability for use in OT, so must any and all threat data within a model or simulation be accredited for its appropriateness and suitability for use in a given OT event. This includes, but is not limited to Ph and Pk tables, Doctrinal Templates, Threat System Characteristics and Performance tables, TTPs, and so forth. Threat Accreditation Working Groups (TAWGs) for M&S must be convened as soon as the T&E WIPT or one of its subordinate IPTs identifies M&S applications to be used in the test.

Y–29. Intelligence Production Centers

Intelligence production centers, such as the National Ground Intelligence Center (NGIC) and the Missile and Space Intelligence Center (MSIC) perform a critical role in providing the T&E community with a realistic threat environment. Intelligence production centers (that is, depending on the threat to be portrayed, NGIC or MSIC) provides the following assistance:

a. Produces and disseminates general military and scientific and technical intelligence used by test planners and evaluators to determine system effectiveness and suitability.

b. Produces intelligence to satisfy regulatory responsibilities that Army systems be tested in a realistic threat environment.

c. Participates in Validation Working Groups and TAWGs to ensure proper threat data are being utilized in the design, development, and fielding of targets and threat simulators/simulations.

d. Participates in TCGs and T&E Threat Working-level IPTs to assist in the integration of the appropriate threat data in test planning and design.